UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/009,840	05/01/2002	Olivier Lenoir	0501-1052	1234

466   7590   10/05/2007
YOUNG & THOMPSON
745 SOUTH 23RD STREET
2ND FLOOR
ARLINGTON, VA 22202

EXAMINER
DINH, MINH

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
10/05/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _02 July 2007_.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-12_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-12_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

Response to Amendment

1.   This action is in response to the RCE/amendment filed 07/02/07.

Claim 1 has been amended.

Response to Arguments

2.   Applicant's arguments with respect to the rejection of claim 1 under 35

USC 103(a) has been fully considered but they are not persuasive.

Applicant argues that Ratayczak (US 6,259,909 B1) does not disclose that

the second codeword provides the user means for generating an

authentication password intended to be transmitted to the server side (page

11, 2nd). Applicant reasons that, in Ratayczak, the second code word is just

transmitted from the second communication device to the first

communication device; however, the process of claim 1 requires a person

who can realize an intellectual step of using the transmitted message as

means for generating an authentication password (page 11, 3rd paragraph).

        Ratayczak discloses that the second code may be transmitted from the

second communication device (e.g., a telephone/mobile phone) to the first

communication device (e.g., a computer) in different ways, at least one of

which requires user interaction, i.e., the second communication device

displays the second word so that it can be input into the first communication

device (col. 7, lines 8-10). It is well known in the art that a landline

telephone cannot transmit data to a computer and vice versa, inherently,

user interaction is always required if the second communication device is a

landline a telephone.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and
> distinctly claiming the subject matter which the applicant regards as his invention.

4.   Claims 1-12 are rejected under 35 U.S.C. 112, second paragraph, as

being indefinite for failing to particularly point out and distinctly claim the

subject matter which applicant regards as the invention. Regarding claims

1, 9-11, it is not clear what the structures corresponding to the means-plus-

function limitations are in the specification.

Claim Rejections - 35 USC § 103

5.   Claims 1-3, 5, 9-10 and 12 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Ratayczak.

Regarding claims 1, 9-10 and 12, Ratayczak discloses a process of

securing the access to a data processing server from a client site through at

least a first communication network, i.e., Internet, this server comprising

means for handling a protocol of authenticating a client site user, i.e., a

person, comprising a sequence of receiving and processing identification

data of a client site user, and a sequence of transmitting a message from

the server site to a client site user owned communication equipment through

a second communication network, i.e., a telephone and a fixed telephone

network, characterized in that this transmitted message providing to the

aforesaid user means for generating an authentication password intended to

be transmitted to the aforesaid server site through either the first or the

second communication network (col. 1, lines 21-28; col. 6, lines 59-67; col.

7, lines 1-23, 36-47), the call number of the aforesaid communication

equipment being searched from an authentication data base (col. 4, lines

12-25).

Ratayczak does not disclose that the message is a voice message.

However, it is well known in the art that not all landline telephones have a

display. Therefore, it would have been obvious to modify Ratayczak's

method such that the message is a voice message since there would be no

other option for landline telephones that do not have a display.

Regarding claim 2, Ratayczak discloses the securing process according

to claim 1, characterized in that it comprises steps of:

requesting identification data (ID, MPC) from the client site through

the first communication network (column 6 lines 59-64);

processing the aforesaid data (ID, MPC) and searching an

authentication database for a client user owned communication equipment

call number (this is inherent in column 7 lines 1-5 and 36-44 in that the

server must know the call number of the mobile device from the HLR

described in column 4 lines 12-24);

calling the aforesaid communication equipment through at least a

second communication network (column 7 lines 1-5 and 36-44);

after establishing a communication with the aforesaid mobile

communication equipment, generating a random or pseudo random

password (MPA) (column 7 lines 36-40);

sending a voice message comprising the aforesaid random password

through the second communication network (column 7 lines 1-5, see also

above);

requesting the user provide, from the client site through the first

communication network an authentication password (7 lines 13-15) derived

from the aforesaid random or pseudo random password; and

authenticating the aforesaid authentication password (column 7 lines

13-15).

Regarding claim 3, Ratayczak further discloses that the authentication

password matches the server generated random or pseudo random

password transmitted through the mobile communication equipment

(column 7 lines 1-13).

Regarding claim 5, Ratayczak further discloses that the identification

data requested from the client consists of a couple [identification code/client

password] (column 6 lines 59-64).

6.   Claims 4 and 6 rejected under 35 U.S.C. 103(a) as being unpatentable

over Ratayczak as applied to claims 3 and 1 above, and further in view of

Guthrie et al. (US 6,161,185).

Regarding claim 4, Ratayczak does not disclose that the authentication

password is built from the random or pseudo random password using a key

shared by the client user and the server. Guthrie discloses method for

generating authentication password, i.e., a one-time password, used in level

two of a two-level authentication protocol wherein the authentication

password used in level two is built, at the client user side, from a random or

pseudo random password generated by the server using a key shared by the

client user and the server (figures 3-4; col. 6, line 10 – col. 7, line 9). It

would have been obvious to one of ordinary skill in the art at the time the

invention was made to incorporate Guthrie's method for generating the one-

time password into Ratayczak's method so that the server could determine

that the password was generated by an entity that knew the shared secret

key.

Regarding claims 6, Guthrie further discloses that the one-time

password is valid only for a short period of time (col. 2, lines 48-53). It

would have been obvious to one of ordinary skill in the art at the time the

invention was made to modify Ratayczak's method such that the one-time

password is valid only for a short period of time, as taught by Guthrie. The

motivation for doing so would have been to foil a malicious user's attempt at

"hammering" the authentication system with response attempting to

stumble upon a correct password and gain access (col. 2, lines 48-53).

7.   Claims 7 and 11 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Ratayczak as applied to claims 1 and 9 above, and further

in view of Kelly (5,636,280).

Ratayczak discloses the securing process according to claim 1,

characterized in that it comprises on the server side the steps of:

requesting identification data (ID, MPC) from the client site through

the first communication network (column 6 lines 59-64);

processing the aforesaid data (ID, MPC) and searching an

authentication database for a client user owned mobile communication

equipment call number (this is inherent in column 7 lines 1-5 and 36-44 in

that the server must know the call number of the mobile device from the

HLR described in column 4 lines 12-24);

calling the aforesaid communication equipment through at least a

second communication network (column 7 lines 1-5 and 36-44);

in case the communication is established with the aforesaid mobile

communication equipment, send a voice message requesting the user to

send an encryption key (Column 4 lines 55-62, wherein the codeword can be

used as an encryption key as stated in column 7 lines 59-62);

receiving and recognizing the encryption key transmitted by the client

by means of the mobile equipment keyboard (column 4 lines 59-65),

Ratayczak does not disclose using the key by the client user side to

encrypt an authentication password transmitted to the server and using the

key by the server to decrypt the encrypted password for authentication.

Kelly discloses an authentication method wherein the user's password is

encrypted using a key shared with a server prior to being transmitted to the

server, and that the server uses the shared key to decrypt the encrypted

password for authentication (fig. 4, steps 126, 128 and 130). It would have

been obvious to one of ordinary skill in the art at the time the invention was

made to modify Ratayczak's method to use the key by the client user side to

encrypt an authentication password transmitted to the server and use the

key by the server to decrypt the encrypted password for authentication, as

taught by Guthrie. The motivation for doing so would have been to protect the password when it was transmitted from the client to the server.

8.   Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ratayczak in view of Kelly as applied to claim 7 above, and further in view of Guthrie. Ratayczak does not disclose that the code word, which is used as the encryption key, is valid only a short period of time. Guthrie further discloses that a one-time password is valid only for a short period of time (col. 2, lines 48-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Ratayczak and Kelly such that the code word is valid only for a short period of time, as taught by Guthrie. The motivation for doing so would have been to foil a malicious user's attempt at "hammering" the authentication system with response attempting to stumble upon a correct password and gain access (col. 2, lines 48-53).

Conclusion

9.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent No. 5,893,830 to Wesinger, Jr. et al.

U.S. Patent No. 6,993,658 to Engberg et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number . is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.
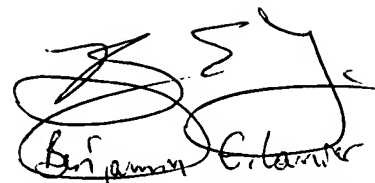
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/
Minh Dinh
Examiner
Art Unit 2132

9/30/07

Examiner AU 2132